AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) A method for pairing a decoder and a portable security module, comprising: ~~a first element and a second element, the first element and the second element forming a first decoding system among a plurality of receiving decoding systems in a broadcasting network, each receiving decoding system being adapted to descramble scrambled audiovisual information received over the broadcasting network, the method comprising~~:

   selecting a first key, the first key being unique in the broadcasting network;

   assigning the first key to the decoder, wherein the decoder and the portable security module form a first receiving decoding system among a plurality of receiving decoding systems in the broadcasting network, wherein each receiving decoding system is configured to descramble scrambled audiovisual data received via the broadcasting network;

   determining a second key according to the first key, such that a combination of the first key and the second key is congruent to a pairing system key, wherein the pairing system key is common to each receiving decoding system and allows for decryption of encrypted control data ~~that is received to be decrypted by each receiving decoding system~~, the encrypted control data being identical for each receiving decoding system;

   assigning ~~respectively the first key and~~ the second key to the portable security module to obtain a pairing of the decoder and the portable security module ~~first element and the second element~~.

2. (Currently Amended) The method according to claim 1, wherein the control data enables to descramble the scrambled audiovisual information, the method further comprising:

   receiving, at the first receiving decoding system, the encrypted control data;

   using the first key at the decoder ~~first element~~ and using the second key at the portable security module ~~second element~~ to decrypt the encrypted control data.

3. (Currently Amended) The method according to claim 1 ~~any one of claims 1~~, wherein the control data is a control word, the audiovisual information being scrambled using the control word.

4. (Currently Amended) The method according to claim 1~~any one of claims 1~~, wherein the control data is an Entitlement Control Message (ECM) comprising a control word, the audiovisual information being scrambled using the control word.

5. (Currently Amended) The method according to claim 1~~any one of claims 1~~, wherein the control data is an exploitation key, the exploitation key enabling to decode a control word, the audiovisual information being scrambled using the control word.

6. (Currently Amended) The method according to claim 1~~any one of claims 1~~, wherein the control data is an Entitlement Management Message (EMM) comprising an exploitation key enabling to decode a control word, the audiovisual information being scrambled using the control word.

7. (Currently Amended) The method according to claim 1 ~~any one of claims 1~~, wherein the encrypted control data is decrypted using a RSA algorithm, the method further comprising, for the RSA algorithm:

selecting a first prime number p and a second prime number q;

calculating a modulus number n as being equal to a product of the first prime number p and the second prime number q;

selecting an encrypting key e as being smaller to the modulus number and as being prime with a function of the first prime number p and the second prime number q;

determine a private key as being equal to an inverse of the encrypting key modulus the function of the first prime number p and the second prime number q;

selecting the first key and the second key such that a product of the first key and the second key equals the private key modulo the function of the first prime number p and the second prime number q;

erasing the first prime number p and the second prime number q.

8. (Currently Amended) The method according to claim 7, further comprising:

receiving, at each of the plurality of receiving decoding systems, a message comprising the encrypted control data;

decrypting the encrypted control data using the first key at the decoder ~~first element~~ and the second key at the portable security module~~second element~~.

9. (Currently Amended) The method according to claim 1~~any one of claims 1~~, wherein the encrypted control data is decrypted using a discrete logarithm[[s]] algorithm, the method further comprising, for the discrete logarithm algorithm:

selecting a prime number q; and

selecting a primitive root of the prime number g[[;]],

[[and]]wherein a product of the first key and the second key equals a private key modulo the prime number.

10. (Currently Amended) The method according to claim 9, further comprising:

receiving, at each of the plurality of receiving decoding systems, a message comprising an encrypted information encrypted with a cession key, the message also comprising the primitive root of the prime number g power a random number k;

using the first key at the decoder ~~first element~~ and using the second key at the portable security module ~~second element~~ to calculate the cession key from the prime number power the random number k;

decrypting the encrypted information using the cession key.

11. (Original) The method according to claim 10, wherein the encrypted information is the scrambled audiovisual information.

12. (Original) The method according to claim 10, wherein the encrypted information is a control word, the audiovisual information being scrambled using the control word.

13. (Currently Amended) The method according to claim 1~~any one of claims 1~~, further comprising respectively attributing the first key and the second key at least to a second decoder and a second portable security module ~~third element and a fourth element~~ forming a second receiving decoding system from the plurality of receiving decoding systems distinct from the first receiving decoding system.

14. (Canceled)

15. (Currently Amended) A first receiving decoding system among a plurality of receiving decoding systems in a broadcasting network, each receiving decoding system being adapted to descramble scrambled audiovisual information received over the broadcasting network, the first decoding system comprising:

a ~~first element~~ decoder to which is assigned a first key, the first key being unique in the broadcasting network;

a ~~second element~~ portable security module to which is assigned a second key, wherein the decoder and the portable security module form a pairing system, and

wherein the second key [[being]] is determined according to the first key such that a combination of the first key and the second key is congruent to a pairing system key which enables [[to]] decryption of broadcasted encrypted control data that is received ~~to be decrypted~~ by each receiving decoding system, the encrypted control data being identical for each receiving decoding system.

16. (Currently Amended) The first decoding system according to claim 15, further comprising:

~~receiving means to receive~~ a receiver for receiving the broadcasted encrypted control data;

a pair of decryptions comprising a first decryption located in the decoder and a second decryption ~~respectively~~ located in the portable security module ~~first element and the second element~~, wherein the pair of decryptions enables[[ing]] [[to]] decryption of the broadcasted encrypted control data using the first key and the second key.

17. (Currently Amended) The first decoding system according to ~~any one of claims~~ claim 15, wherein the broadcasted encrypted control data is decrypted using a discrete logarithm algorithm.

18. (Currently Amended) The first decoding system according to ~~any one of claims~~ claim 15, wherein the broadcasted encrypted control data is decrypted using a RSA algorithm.

19. (Currently Amended) The first decoding system according to ~~any one of claims~~ claim 15, wherein the control data is a control word, the audiovisual information being scrambled using the control word.

20. (Currently Amended) The first decoding system according to ~~any one of claims~~ claim 15, wherein the control data is an exploitation key, the exploitation key enabling to decode a control word, the audiovisual information being scrambled using the control word.

21. – 22. (Canceled)